UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,849	07/03/2001	Todd A. Anderson	42390P11768	1484

8791 7590 04/20/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/898,849	ANDERSON ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-11,13-20,22-27 and 29-35* is/are rejected.

7)☒ Claim(s) *7,12,21 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 12/27/2004. Claims 1-5, 7, 11-13, 15-29 and 33 have been amended. The drawings have also been amended.

Response to Arguments

2. Applicant's arguments filed 12/27/2004 have been fully considered but they are not persuasive. The subject matter indicated as allowable in the previous Action was not fully incorporated into the independent claims. The Smith reference does show a pre-programmed squelch time to live value used by the upstream router to define an expiration time for the received filter (Sections 3.1, Filter & Monitor Requests; 3.2, Relay Feature). Since the amended independent claims does not specify where or by whom the squelch time to live value was generated, they do not distinguish over the prior art.

Applicant argues that Smith fails to teach that an Internet host receives notification of a DDoS attack (p. 14). Smith discloses that a corporate firewall receives notification of a DDoS attack (p. 76, right col., 1st and 2nd paragraphs); the corporate firewall constitutes an Internet host.

Claim Objections

3. Claim 4 is objected to because of the following informalities: "a digital certificate or the Internet host". Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6, 8-10, 15-20, 22-27 and 29-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith et al. ("A Protocol and Simulation for Distributed Communicating Firewalls") in view of Shyne et al. ("Using Active Networking to Thwart Distributed Denial of Service Attacks").

Regarding claims 1-2 and 15-16, Smith discloses a method comprising: receiving, by a corporate firewall, which meets the limitation of an Internet host, a notification of a denial of service attack (p. 76, right col., 1st par.; p. 77, left col. 3rd par.); establishing security authentication with an upstream router from which attack traffic, transmitted by one or more attack host computers, is received (figures 1 and 2); and once security authentication is established, transmitting one or more filters to the upstream router such that attack traffic is dropped by the upstream router to terminate the denial of service attack, wherein the upstream router includes a pre-programmed squelch time to live value used by the upstream router to define an expiration time for the one or more filters (Sections 3.1, Filter & Monitor Requests; 3.2, Relay Feature). Smith does not disclose detecting a distributed denial of service attack. Shyne discloses detecting a distributed denial of service attack by monitoring network traffic

received by a host and notifying the host of the distributed denial of service attack (p. 3-1106, see Detection Mechanisms). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Smith method such that it can detect a distributed denial of service attack, as taught by Shyne. A distributed denial of service attack cannot be dealt with unless it is detected first.

Regarding claims 3 and 17, Smith further discloses transmitting a security authentication request to the upstream router including authentication information, the authentication information including a destination address of the attack traffic and receiving authorization for establishment of security authentication from the upstream router (fig. 1; p. 77, left col., 3rd and 4th paragraphs).

Regarding claims 4 and 18, Smith further discloses identifying attack traffic characteristics of the attack traffic received by an Internet host; generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics; digitally signing the one or more filters; and transmitting the one or more digitally signed filters to the upstream router (p. 77, right col., 3rd par). Smith does not disclose sending the digital certificate of the Internet host with the signed filters. However, Examiner takes Official Notice that sending the digital certificate of the signer with a signed document is well known in the art. It would have been obvious at the time of the invention was made to send the digital certificate of the Internet host with the signed filters since Examiner takes Official Notice that sending the digital certificate of

the signer with a signed document to facilitate digital signature verification is well known in the art.

Regarding claims 5, 8, 19, 22, 26, 29 and 33-34, Smith discloses a method comprising: establishing security authentication of a corporate firewall, which meets the limitation of an Internet host, under a denial of service attack (p. 76, right col., 1st par.; p. 77, left col. 3rd par.); receiving one or more filters from the Internet host (p. 77, right col., 3rd par); generating a filter expiration time for each filter based on a pre-programmed squelch time to live value (Sections 3.1, Filter & Monitor Requests; 3.2, Relay Feature); when security authentication is established, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the Internet host (p. 77, right col., 3rd par). Smith does not explicitly disclose verifying that the one or more filters select only network traffic directed to the Internet host. However, this feature is deemed to be inherent to the Smith method as the 1st paragraph in the right column of page 77 shows that each Communicating Gateway Firewall Protocol (CGFP) router keeps track of the number of filters for each Internet host. Since the destination address information in each filter (p. 77, right col. 3rd par.) is the only information that can be used to associate the filter with an Internet host, the Smith method would be inoperative if the CGFP router did not verify the destination address information in the filter against the Internet host address. Smith does not disclose that the Internet host is able to detect a distributed denial of service attack. Shyne discloses different detection mechanisms for identifying a distributed denial of service attack (p. 3-1106, Detection Mechanisms). It would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the Smith method to apply a detection mechanism to identify a distributed denial of service attack, as taught by Shyne. A distributed denial of service attack cannot be dealt with unless it is detected first.

Regarding claims 6, 23 and 32, Smith further discloses that establishing security authentication further comprises: receiving a request for security authentication including authentication information from the Internet host; selecting the authentication information from the security authentication request; and authenticating an identity of the Internet host based on the selected authentication information (fig. 1).

Regarding claims 9, 24 and 30, Smith further discloses selecting network traffic matching one or more of the filters received from the Internet host; and dropping the selected network traffic such that attack traffic received from one or more attack host computers by the Internet host is eliminated in order to terminate the distributed denial of service attack (p. 77, right col., 3rd par).

Regarding claims 10, 25, 31 and 35, Smith further discloses determining, by an upstream router receiving the one or more filters from the Internet host, one or more ports from which the attack traffic matching the one or more filters is being received based on a routing table (p. 77, right col., 3rd par.), selecting a port from the one or more determined ports, determining an upstream router connected to the selected port based on a routing table, securely forwarding the one or more filters received from the Internet host to the detected upstream router as a routing protocol update; and repeating the selecting, determining and utilizing for each of the one or more determined ports (p. 78, left col., 2nd par).

Regarding claims 20 and 27, Smith further discloses that establishing security authentication comprises: receiving a routing protocol update from the downstream device; selecting authentication information from the received routing protocol update; authenticating an identity of the downstream device based on the selected authentication information; once authenticated, selecting the one or more filters from the received routing protocol update; and authenticating integrity of the one or more filters based on a digital signature of the filters (Section 2.1, Border Gateway Protocol; p. 77, left col., first and third paragraphs).

6. Claims 11 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith in view of Hardjono (6,425,004).

Regarding claim 11, Smith discloses a method comprising: receiving a routing protocol update from a downstream router (Section 2.1, Border Gateway Protocol); selecting one or more filters from the routing protocol update received from the downstream router (p. 78, left col., 2nd par); establishing security authentication of the downstream router (fig. 1); generating a filter expiration time for each filter based on a pre-programmed squelch time to live value, such that the filters are uninstalled once the expiration time expires (Sections 3.1, Filter & Monitor Requests; 3.2, Relay Feature); once authentication is established, installing the one or more filters such that attack traffic matching the one or more filters is prevented from reaching the downstream router (p. 78, left col., 2nd par). Smith does not disclose verifying that the one or more filters select only network traffic directed to the downstream router. Hardjono discloses

that when a first router receives routing information, which meets the limitation of filtering information, from a second router, the first router not only authenticates the routing information but also verifies that the routing information is consistent with other routing information previously received by the first router (col. 1, lines 54-63; col. 5, line 61 – col. 6, line 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Smith method such that the upstream router verifies the filter information received from the downstream router against previously received routing information, as taught by Hardjono, in order to avoid performance degradation due to invalid routing information (col. 1, lines 48-54). Accordingly the upstream router should verify that the destination address component of the filter should match one entry in its routing table.

Regarding claim 13, Smith further discloses verifying that the downstream router is a next hop router according to a routing table (Fig. 2; Section 3.2, Relay Feature).

Regarding claim 14, Smith further discloses determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received; selecting a port from the one or more determined ports; determining an upstream router coupled to the selected port based on a routing table; securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and repeating the selecting, determining, and forwarding for each of the one or more determined ports (Section 3.1, Filter & Monitor Request; Section 3.2, Relay Feature).

Allowable Subject Matter

7. Claims 7, 12, 21 and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. Regarding claims 7, 12, 21 and 28, the limitations "once authenticated, verifying that a router administrator has programmed a DDOS squelch time to live value for received filters; verifying that an action component of each of the filters is drop; and otherwise, disregarding the one or more filters received from the Internet host/downstream device" in combination with elements of the parent claims have not been taught by prior art.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MP

Minh Dinh
Examiner
Art Unit 2132

MD
4/14/05

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100